

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PERSON
OF DONALD SCHWARTZ, THE PREMISES KNOWN
AS 22 GORDON DRIVE LONDONDERRY, NH, ONE
2021 GRAY HYUNDAI SANTA FE BEARING NEW
HAMPSHIRE REGISTRATION "MOODLE," AND ANY
COMPUTER, COMPUTER MEDIA OR ELECTRONIC
STORAGE FOUND IN THE PREVIOUS
LOCATIONS

Case No. 23- mj-226-01/03-TSM

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Marvin Alfaro, a Task Force Officer with the United States Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating the offenses of distribution and possession of child pornography via the peer-to peer ("P2P") network BitTorrent, by an individual(s) using the internet service assigned to 22 Gordon Drive, Londonderry, NH ("SUBJECT PREMISES"). As will be shown below, there is probable cause to believe that Donald Schwartz ("SCHWARTZ"), who appears to be the owner and sole occupant of the SUBJECT PREMISES, has committed the offenses of distribution and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2), and 2252A(a)(5)(B). I submit this affidavit in support of an application for a warrant under Rule 41 of the Federal Rules of Criminal Procedure to search the SUBJECT PREMISES, the person of Donald Schwartz ("SCHWARTZ"), and a gray 2021 Hyundai Santa Fe bearing NH registration MOODLE ("SUBJECT HYUDAI"), further described in Attachment A and incorporated herein by reference, for evidence, fruits, and instrumentalities of the forgoing criminal violations. I specifically request authority to search the SUBJECT PREMISES, the person of SCHWARTZ, and the SUBJECT HYUNDAI, for any computer and computer media located therein where the items specified in

Attachment B, incorporated herein by reference, may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of criminal activity.

2. This affidavit is based in part on information that I learned from discussions with other law enforcement officers and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the evidence, fruits, and instrumentalities of the violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B), will be located within the SUBJECT PREMISES, on the person of SCHWARTZ, and/or within the SUBJECT HYUNDAI.

OFFICER BACKGROUND

3. I am currently a detective with the Londonderry New Hampshire Police Department, where I have been employed since December of 2018. I became a certified police officer in the state of New Hampshire in April 2019 through the New Hampshire Police Standards and Training Council as a graduate from the 178th full time police academy class. I hold a bachelor's degree from Villanova University in Pennsylvania with majors in Finance and Accounting. I am also currently a Task Force Officer (TFO) with HSI and assigned to the Manchester, NH field office. I completed the HSI Task Force Officer Course in August 2023.

4. As part of my duties as a TFO with HSI, I am authorized to investigate criminal violations relating to a broad range of immigration and customs-related statutes, including those relating to child exploitation and child pornography. As a Londonderry Police Officer, I have received training in the area of child pornography and child exploitation, and as part of my law enforcement duties, have observed and reviewed numerous examples of child pornography (as defined in NH RSA 649-A and in 18 U.S.C. §2256) in various forms of media, including

digital/computer media. Additionally, I have conducted investigations and assisted in the execution of search warrants involving child exploitation and child pornography offenses.

SPECIFIED FEDERAL OFFENSES

5. Title 18, United States Code, Section 2252A(a)(5)(B) prohibits a person from knowingly possessing or accessing with intent to view any material that contains an image of child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. Title 18, United States Code, Section 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this affidavit and Attachment B:
- a.) “Child pornography” includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from , that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).
 - b.) “Child Erotica,” as used herein, means material or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.
 - c.) “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).
 - d.) “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

- e.) “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile “smart” telephones, tablets, and self-contained “laptop” or “notebook” computers).
- f.) “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- g.) “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h.) The “internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- i.) “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.
- j.) The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing), or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMS, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards,

memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON PEER-TO-PEER (“P2P”) SOFTWARE

7. Peer-to-peer (“P2P”) file-sharing is a method of communication available to Internet users through the use of special software such as BitTorrent. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in shared folder its distribution is dependent only on the machine being turned on and connected to the Internet.

8. BitTorrent is one type of P2P file-sharing protocol. Users of the BitTorrent network wishing to share new content will use a BitTorrent client to create a “torrent” file of the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their “infohash,” which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software

processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

9. One of the advantages of P2P file-sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

10. The BitTorrent network bases all of its file shares on the Secure Hash Algorithm (“SHA1”). This mathematical algorithm allows for the digital fingerprinting of data by assigning a fixed-length unique identifier known as SHA1 value (i.e., a “digital fingerprint”) to a digital file. The SHA1 is secure and reliable because it is computationally infeasible for two files with different content to have the same SHA1 value.

PROBABLE CAUSE

11. This investigation was initiated through the use of investigative BitTorrent software that identifies SHA1 hash values of torrents being shared on the BitTorrent network that have been previously determined to contain child pornography and/or related material. When the software recognizes a SHA1 hash value for a torrent that contains such files on the network, it automatically tries to download the torrent. Further, the BitTorrent software used by law enforcement uses a single-source download protocol. In other words, when the software identifies a BitTorrent user that has suspected files of child pornography available for download, it will initiate a

download of the entire file from that single user, as opposed to downloading portions of the target file from multiple users.

12. On May 13, 2023, the investigative BitTorrent software identified a torrent with a SHA1 value of investigative interest available for download from a device utilizing IP address 75.68.28.65. This torrent file references 57,756 files, at least one of which was identified as being a file of investigative interest to child pornography investigations. A computer running the investigative BitTorrent software made a direct connection to the device utilizing IP address 75.68.28.65 and between May 13, 2023 at 1444 hours and May 14, 2023 at 0753 hours, a download was successfully completed of 56,594 files that the device utilizing IP address 75.68.28.65 was making available. The device utilizing IP Address 75.68.28.65 was the sole candidate for the download, and as such, the files were downloaded directly from that device. One of the downloaded files is described as:

File Name: lsm13-04-02.mpeg

Description: This video file is approximately 5 minutes and 1 second in length. It shows two prepubescent naked females wearing high heeled shoes. The camera zooms in on the blonde female's vagina as she sits on a chair. Later in the video, both females are seen pouring an unknown yellow colored substance from a cup onto their breasts and down to their vaginas. Both females have no visible breast development and lack pubic hair. The video later shows the blonde female bend over as the camera zooms in on her vagina.

13. On July 14, 2023, the investigative BitTorrent software identified a torrent with a SHA1 value of investigative interest available for download from a device utilizing IP address 75.68.28.65. This torrent references 1 file, which was identified as being a file of investigative interest to child pornography investigations. A computer running the investigative BitTorrent software made a direct connection to the device utilizing IP address 75.68.28.65 and between 2216 and 2217 hours, a download was successfully completed of 1 file that the device utilizing IP address

75.68.28.65 was making available. The device utilizing IP Address 75.68.28.65 was the sole candidate for the download, and as such, the file was downloaded directly from that device. The downloaded file is described as:

File Name: [JulyJailbait] - [jjclubumn7vkhyuw.onion] - Polarlights studio - Quartet2
part1 .mp4

Description: This video is approximately 15 minutes 5 seconds in length. It shows a naked prepubescent male with no pubic hair squatting down and laying down on his back. A prepubescent female enters the frame and begins stroking the boy's penis with her hands before placing it inside her mouth. The female then gets on top of the male and his penis goes inside her vagina. Later on, a second prepubescent female enters the frame and puts the boy's penis inside her mouth as the other female looks on.

14. On August 28, 2023, the investigative BitTorrent software identified a torrent with a SHA1 value of investigative interest available for download from a device utilizing IP address 75.68.28.65. This torrent references 1 file, which was identified as being a file of investigative interest to child pornography investigations. A computer running the investigative BitTorrent software made a direct connection to the device utilizing IP address 75.68.28.65 and between 1954 and 2010 hours, a download was successfully completed of 1 file that the device utilizing IP address 75.68.28.65 was making available. The device utilizing IP Address 75.68.28.65 was the sole candidate for the download, and as such, the file was downloaded directly from that device. The downloaded file is described as:

File Name: Yvm_ Young Video Models - Seven days with Masha-FULL-THE BEST.avi

Description: This video file is approximately 1 hour 28 minutes and 44 seconds in length. The video depicts a juvenile female with no visible breast development and minimal pubic hair. The same juvenile female appears in multiple segments through the video, each representing a different "day" as described below:

Day 1: Begins at 00:01. The female is outdoors and undresses while leaning up against a tree. The video zooms into her exposed vagina multiple times.

Day 2: Begins at 02:59. The female is outdoors and undresses while laying on a towel in a grass field. The video zooms into her exposed vagina multiple times.

Day 3: Begins at 15:13. The female fully undresses and gets into a bathtub. The female inserts a Q-Tip and fingers into her vagina. The hand of an adult male is then seen applying lubrication on her anus and then inserts a tubular device inside her anus. The male then penetrates the female's vagina with his finger.

Day 4: Begins at 34:17. The female completely undresses and lays naked on her back on top of a bed. She rubs and penetrates her vagina using her finger.

Day 5: Begins at 45:45. The female enters the back seat of a vehicle and removes her lower garments. She lays down on the car seat and penetrates her vagina with her finger.

Day 6: Begins at 59:10. The female fully undresses in the same bedroom as "Day 4." She penetrates her vagina with her finger while laying on her back on top of the bed.

Day 7: Begins at 1:12:14. The female fully undresses in the same bedroom. She lays down on the bed and penetrates her vagina with her finger. An adult male's arm is seen and he penetrates the female's vagina with his finger.

15. On September 16, 2023, the investigative BitTorrent software identified a torrent with a SHA1 value of investigative interest available for download from a device utilizing IP address 75.68.28.65. This torrent file references 1 file, which was identified as being a file of investigative interest to child pornography investigations. A computer running the investigative BitTorrent software made a direct connection to the device utilizing IP address 75.68.28.65 and between 2226 and 2233 hours, a download was successfully completed of 1 file that the device utilizing IP address 75.68.28.65 was making available. The device utilizing IP Address 75.68.28.65 was the sole candidate for the download, and as such, the file was downloaded directly from that device. The downloaded file is described as:

File Name: bd-company full (Series 1 of beautiful pretty TANYA).avi

Description: This video is approximately 59 minutes 58 seconds in length. It shows a prepubescent female with no pubic hair or breast development wearing high heeled shoes posing

various positions throughout the video to include multiple poses with her legs fully spread exposing her vagina.

16. On November 1, 2023, an administrative summons was served to Comcast Cable Communications LLC requesting subscriber information for IP address 75.68.28.65 assigned on May 13, 2023 at 1444 hours EST, July 14, 2023 at 2216 hours EST, and on August 28, 2023 at 1954 hours EST. On November 3, 2023, Comcast responded to the Summons, and provided the following subscriber information:

Subscriber Name:	Donald Schwartz
Service & Billing Address:	22 Gordon Drive, Londonderry, NH 030532920
Telephone #:	(603) 432-3078

17. The information provided in the response to the summons also indicated that IP address 75.68.28.65 was assigned to this account beginning on June 25, 2020, and was active as of the date of the summons issued of November 3, 2023.

18. According to property assessment data for Londonderry, NH, the SUBJECT PREMISES is owned by SCHWARTZ and Dian J. Schwartz. According to an online obituary I found as part of this investigation, I learned that Dian Schwartz passed away in December 2020.

19. According to the New Hampshire Division of Motor Vehicles, SCHWARTZ holds an active New Hampshire Drivers License, issued on May 6, 2020. SCHWARTZ's address is listed as the SUBJECT PREMISES.

20. Between the months of July and December 2023, I conducted intermittent surveillance on the SUBJECT PREMISES at various days of the week and times of day. On multiple occasions, I observed the SUBJECT HYUNDAI parked on the residence's front driveway.

21. According to the New Hampshire Division of Motor Vehicles, the SUBJECT HYUNDAI (VIN# KM8S2DA14MU006086) is registered to SCHWARTZ as the primary registered

owner and Hyundai Lease Titling Trust as the second registered owner. The registration address on the vehicle is the SUBJECT PREMISES. While conducting surveillance on the SUBJECT PREMISES, I have not seen any other vehicle besides the SUBJECT HYUNDAI at the SUBJECT PREMISES.

22. Through review of open-source and law enforcement databases, it appears that SCHWARTZ has at least two adult children who reside outside the state of New Hampshire. This information is unconfirmed.

23. Based on the investigation to date, it appears that SCHWARTZ resides at the property alone; however, this information is unconfirmed. This conclusion is based on a review of open source and law enforcement databases as well as the absence of any other vehicles or people observed at the SUBJECT PREMISES during intermittent physical surveillance.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

24. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced, possessed, distributed, and stored.

25. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking. With digital cameras, images of child pornography can be taken with or transferred directly onto a computer. In addition, the use of commercially available software and devices also allows for the conversion and transfer of other forms of visual media into various digital and electronic media formats. A modem allows any

computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the internet, electronic contact can be made to millions of computers around the world.

26. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. This is also true for portable electronic devices like cell phones and tablets.

27. The Internet affords users several different venues for meeting and communicating with each other and for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. The Internet is also used as a means for child sexual exploitation offenders to solicit potential victims through the use of various online services to include, but not limited to, online profiles, email, instant messaging, and chat.

28. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP ("Internet Service Provider") client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet History files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

29. Computer files or remnants of files can be recovered months or years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer or portable electronic device, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

30. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

31. File transfers and online connections occur to and from IP (“Internet Protocol”) addresses. These addresses are unique to particular computers during online sessions. An IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.

32. Third-party software is available to identify the IP address of a particular computer during an online session. Such software monitors and logs Internet and local network

traffic. It is possible to identify the person associated with a particular IP address through Internet Service Provider Records. ISPs maintain records of the IP addresses used by the individuals or businesses that obtain Internet connection service through the ISP. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

33. Searches and seizures of evidence from computers commonly require investigators to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

- a.) Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Additionally, when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days, weeks, or months, depending on the volume of data stored, and is generally difficult to accomplish on site.
- b.) Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

34. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (“CPU”). In cases involving child

pornography where the evidence consists partly of graphic files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating system or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

35. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes within the meaning of 18 U.S.C. Sections 2252A(a)(2) and (a)(5)(B), they should all be seized as such.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS:

36. As described above and in Attachment B, this application seeks permission to search and seize certain records that might be found within the SUBJECT PREMISES, on the person of SCHWARTZ, and/or within the SUBJECT HYUNDAI. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure and search of any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found during the course of said searches, and potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

37. I submit that if a computer or other electronic storage medium is found within the SUBJECT PREMISES, on the person of SCHWARTZ, and/or within the SUBJECT HYUNDAI, there is probable cause to believe those records will be stored on that computer or electronic storage medium, for at least the following reasons:

- a.) Based on my knowledge, training, and experience, and that of other agents and computer forensic examiners with whom I have conferred, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic

files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b.) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file, for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c.) Wholly apart from user-generated files, computer storage media, in particular, computers’ internal hard drives, contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d.) Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or “cache.”
- e.) I am also aware, through my own training and experience and that of other agents with whom I have conferred, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.
- f.) I am aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize “cloud” storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. I am aware that some smartphones also back up their contents automatically to devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic

and media storage devices via Bluetooth or wireless, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

CHARACTERISTICS OF CHILD PORNOGRAPHY OFFENDERS

38. As set forth above, probable cause exists to believe that an individual that resides at or has access to the SUBJECT PREMISES has distributed, received, and/or possessed child pornography. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

- a.) Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media. Such individuals often times use these materials for their own sexual arousal and gratification.
- b.) Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes, often possess and maintain copies of child pornography material, in the privacy and security of their home or some other secure location.
- c.) Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is highly valued.
- d.) Those who distribute, receive, and/or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

39. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant,

but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer on the SUBJECT PREMISES, on the person of SCHWARTZ, and/or within the SUBJECT HYUNDAI because:

- a.) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file)/. Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b.) Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.
- c.) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d.) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium at are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e.) Further, in finding evidence of how a computer was used, the purpose of its use, who used it and when, it is sometimes necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

40. Based on my training and experience, I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable and often contain a wealth of highly personal and confidential information that individuals have an interest in safeguarding. This includes, by way of example, extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles, and/or on their person.

41. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a.) **The nature of evidence:** As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been

deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

- b.) **The volume of evidence:** Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months to complete, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on site.
- c.) **Technical Requirements:** Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data onsite. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- d.) **Variety of forms of electronic media:** Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

42. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image/copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

43. This warrant seeks authorization for law enforcement to compel SCHWARTZ to unlock devices requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

44. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to use.

45. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up numerous fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

46. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front facing camera then analyzes, and records data based on the user’s facial characteristics. The device can then be unlocked if the front-

facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

47. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light towards the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

48. Users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents.

49. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

50. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric

features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain time period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours have elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for eight hours and the passcode or password has not been entered in the last six days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

51. In light of the foregoing, and with respect to any device seized, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of SCHWARTZ to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of SCHWARTZ and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of SCHWARTZ and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

52. The proposed warrant does not authorize law enforcement to compel SCHWARTZ to state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel SCHWARTZ to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

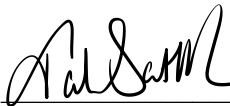

CONCLUSION

53. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crimes of distribution and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2), and 2252A(a)(5)(B) will be located within the SUBJECT PREMISES, on the person of SCHWARTZ, and/or within the SUBJECT HYUNDAI. I therefore seek a warrant to search the SUBJECT PREMISES, the person of SCHWARTZ, the SUBJECT HYUNDAI, and any computers and electronic storage media found therein, as further described in Attachment A, and to seize and search the items described in Attachment B.

Attested to by the Affiant:

/s/ Marvin Alfaro
Marvin Alfaro, Task Force Officer
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P.41 and affirmed under oath the contents of this affidavit and application.



Hon. Talesha L. Saint-Marc
United States Magistrate Judge
Date: December 13, 2023

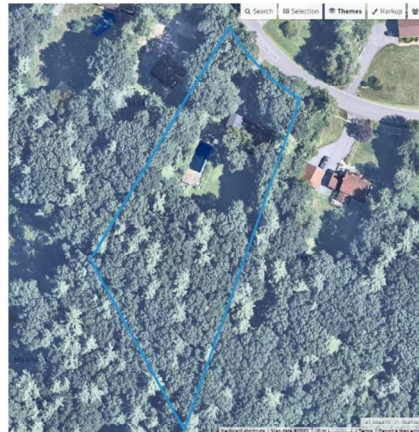
ATTACHMENT A
LOCATIONS AND PERSON TO BE SEARCHED

- 1) The SUBJECT PREMISES is a single-family home located at 22 Gordon Drive, Londonderry, NH 03053, to include all rooms, attics, closed containers, and other places therein, including garages, storage areas, utility sheds, outbuildings, and curtilage. The SUBJECT PREMISES is depicted in the images below. The mailbox at the end of the residence's driveway displays "22."

Figure 1: 22 Gordon Drive- Street View



Figure 2: 22 Gordon Drive- Aerial View



- 2) The person of Donald Schwartz.
- 3) A 2021 Hyundai Santa Fe color gray bearing NH registration MOODLE ("SUBJECT HYUNDAI").
- 4) Any computer, computer media, or electronic storage media found in any of the above locations.

ATTACHMENT B
ITEMS TO BE SEIZED

The items to be seized includes all information and objects that constitute fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) distribution of child pornography and 2252A(a)(5)(B) possession of child pornography, in any form wherever they may be stored or found within the SUBJECT PREMISES, on the person of SCHWARTZ, and/or within the SUBJECT HYUNDAI, including:

1. Computers¹ or storage medium² used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
 - a.) Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b.) Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c.) Evidence of the lack of such malicious software;
 - d.) Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
 - e.) Evidence indicating the computer user’s knowledge and/or intent as it relates to the crime(s) under investigation;
 - f.) Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

¹ The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware

² The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, compact discs, memory cards, memory chips, and other magnetic or optical media

- g.) Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h.) Evidence of the times the COMPUTER was used;
 - i.) Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j.) Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k.) Records of or information about Internet Protocol addresses used by the COMPUTER;
 - l.) Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m.) Contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
 - 4. Child pornography, child erotica, and other images of children, including photographs, drawings, sketches, fantasy writings, and notes showing an interest in unlawful sexual contact with children, and evidence assistance authorities in identifying any such children;
 - 5. Internet history, including evidence of visits to websites and applications that offer visual depictions of minors engaged in sexually explicit conduct or that offer a platform to communicate with others who are interested in unlawful sexual contact with children, including evidence of P2P file sharing programs including BitTorrent;
 - 6. Correspondence and records regarding engaging in, or enticing others to engage in sexually explicit conduct with minors, including envelopes, letters, mailings, electronic mail, chat logs, electronic messages on messaging applications, books, ledgers, and records of communications with other individuals, including on any child exploitation bulletin boards, chat forums, or organizations;
 - 7. Records, information, and items relating to the occupancy of the SUBJECT PREMISES; and
 - 8. Records, information, and items relating to the ownership or use of computer equipment found, including sales receipts, bills for Internet access, and handwritten notes.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

Biometric Access: During the execution of the search of the SUBJECT PREMISES, the person of SCHWARTZ, and/or the SUBJECT HYUNDAI, as described further in Attachment A, law enforcement personnel are authorized to: (1) press or swipe the fingers (including thumbs) of SCHWARTZ to the fingerprint scanner of the devices; (2) hold the devices in front of the face of SCHWARTZ and activate the facial recognition feature; and/or (3) hold the devices in front of the face of SCHWARTZ and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.